New Face of Security: Remember When All We Had to Worry About Were Modems?

by Ed Pierson and Dan Martin

It is terrible when we begin to turn into our parents. Suddenly, all those catch phrases we swore we would never use begin to creep into our conversations with our kids.

This is happening to security professionals. As many healthcare managers and executives spend huge amounts of time and money fighting to protect their systems against external threats, security professionals find themselves harking back to topics that seemingly belong to an earlier generation: physical safeguards and internal risk.

Prior to the PC, information security focused on IDs, passwords, and securing physical files. When PCs first became commonplace, security managers made sure physical doors were secure and identified modems that were plugged into PCs running remote software such as PCAnywhere. In the late ’80s and ’90s, all those PC entry points started letting in worms, viruses, and hackers. The bulk of security measures turned to keeping external people and viruses out of our internal systems.

Understanding a New Wave of Issues

An interesting shift is occurring, raising issues from the early days of the PC. More attention is being focused on protecting against data flowing out of organizations. HIPAA, the Sarbanes-Oxley Act, and other regulations are forcing many security teams to reexamine their organizations’ exposure. Security is no longer simply about keeping hackers from gaining access to patient data, it’s also about putting into place systems that secure and control internal access to information. For example:

- Keeping employees from exposing personal health information (PHI) using instant messaging or personal e-mail accounts
- Preventing visitors from using camera phones to photograph charts left out on counters
- Monitoring data feeds from outside labs to ensure security
- Securing e-mail when doctors discuss diagnosis decisions
- Ensuring systems do not have spyware installed that reports on system activity
- Monitoring traffic to ensure no one is listening in on the wireless network
- Using reverse firewalls that watch for outbound traffic the same as inbound traffic

Then we get back to issues of the past and the questions our predecessors raised. How do we secure our physical data sources? Where do those physical records end up? Often in the trash. And sometimes they don’t remain there for long.

Dumpster Diving—The Latest Threat

The term for digging through trash looking for items of value is “dumpster diving.” Dumpster diving has been around for as long as folks have put their trash out at the curb, but normally it was focused on picking up a perfectly good piece of luggage that your neighbor decided to toss away. Now, thanks to the Internet, it is a major sport.

Do a Google search for the term “dumpster diving” and you’ll find numerous Web sites devoted to local “diving groups” as well as sites for buying and selling the information you find. Books and even forum discussion groups on dumpster diving are readily available. Welcome to the world of the Internet and eBay, where anyone can sell the treasure that was someone else’s trash.

If in your dive you come across a list of e-mail addresses for the employees at a major company, there are people who will pay you for that information. If you come up with the names, addresses, and phone numbers of a thousand patients, that also has a price. What was once a narrow market is now wide open. There is huge demand for information that will allow someone to steal an identity and then defraud a credit card company.

Surely it is illegal to engage in such activities that are obviously such an invasion of privacy? While some cities have tried to enact laws about diving, the US Supreme Court has stated that garbage left at a curb for pick-up is public domain and subject to inspection and seizure by anyone.

The impact of not securing your paper records is potentially huge. *The Seattle Times* reported in June 1999 on a man who during a two-year period found more than 10,000 medical records behind abortion clinics. He sent letters to the patients telling them how he had found their records.[1]

The Impact on Healthcare Organizations

Security departments are now faced with an ever-growing challenge that will only increase with time. Politicians are adding to the challenge by enacting laws that levy significant penalties if someone breaks into or dives into your data and you fail to notify individuals who are potentially at risk. Many senior executives running our organizations are not in tune with the changing risks and exposure, and there is a lack of urgency among our customers because they are just beginning to see the risks as more and more instances of identity theft are exposed in the media.

So what should be done? First, start an awareness campaign to educate your employees. Back it up with your own series of dives into your company's cubicles and office trash bins. Pick up all the leftover documents that accumulate in conference rooms and spend a few minutes looking at what you find. Present the results of your dive to the management team, along with a review of laws like California Senate Bill 1386 (also known as the Database Security Breach Notification Act), HIPAA, the Gramm-Leach Bliley Act, and Sarbanes-Oxley. If you have international operations, present some of the changes on privacy being enforced by the European Union.

Make sure you have shredding bins near your major printers so that employees can securely dispose of misprinted documents rather than dropping them in the nearest trash can. Create a process for properly disposing of floppy disks and CDs that contain key data files. Don't forget about those hard drives in PCs that you get rid of. Make sure they are wiped clean. Educate employees to follow these practices with their personal information at home for all the same reasons your company is promoting them.

Taking the Next Steps

The problem of ensuring the security of your organization's information can best be tackled using both long- and short-term approaches. For the short term:

- Conduct your own dives at your facility to gauge improper data and document disposal
- Educate your IT and executive teams by posting articles about legal liability associated with improper disposal
- Put shredding bins around your office and encourage their use
- Sponsor a competition by rewarding groups that patrol and clean up their own areas

For the long term:

- Join forces with your legal group by getting them to help drive recognition of the issue with the executive team
- Locate and purchase technology that will track and report outbound PHI violations, not just provide inbound protection against viruses
- Educate the general work force on the organizational risks if patient data is compromised

Do not underestimate the challenge of education in terms of security. A 2004 study by Infosecurity Europe in Britain showed that 71 percent of people questioned on the street revealed their commonly used passwords for a bar of chocolate.[2]

Notes

1. "Man Ordered to Return 10,000 Abortion Records." *Seattle Times*, June 10, 1999.

2. Wagner, Mitch. “Will Trade Passwords for Chocolate.” *Security Pipeline*, April 19, 2004. Available online at www.securitypipeline.com/news/18902074.

Ed Pierson *(epierson@healthvision.com) is the chief information officer and vice president and* ***Dan Martin*** *is the director of security for HealthVision in Irving, TX.*

Article citation:
Pierson, Ed, and Dan Martin. "The New Face of Security." *Journal of AHIMA* 76, no.1 (January 2005): 52-53,59.